

Bitte ein Bitcoin – staatlicher Millionengewinn aus beschlagnahmten Bitcoins?

 www.juwiss.de/13-2018/

von JUDITH SIKORA

Auf dem bisherigen Höchststand des Bitcoins-Kurses Mitte Dezember 2017 kündigte die Generalstaatsanwaltschaft Frankfurt an, sie wolle 126 beschlagnahmte Bitcoins (damaliger Wert: 1,9 Millionen Euro) veräußern. Die in Gießen angesiedelte Außenstelle der hessischen Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität ZIT hatte 2014 mehrere Online-Marktplätze abgeschaltet, auf denen u.a. mit Drogen gehandelt wurde. Bei einer Razzia beschlagnahmte sie die Server der Betreiber und gelangte so in den Besitz von Bitcoins. Im Folgenden wird erläutert, wie eine die Beschlagnahme bzw. Sicherstellung von Bitcoins strafprozessual und polizeirechtlich umgesetzt wird und warum die erhofften Millionengewinne die Ausnahme bleiben werden.



Was sind Bitcoins eigentlich?

Bei Bitcoin als prominentestem Vertreter von Kryptowährungen handelt es sich um ein dezentral organisiertes Zahlungssystem mit digitalen „Geld“-Einheiten. Das Bitcoin-Zahlungssystem funktioniert anders als herkömmliche Währungen nicht über eine übergeordnete Abwicklungsstelle (z.B. eine Zentralbank), sondern wird autonom in einem peer-to-peer-Netzwerk organisiert, wobei die Autorisierung mittels kryptografischer Techniken erfolgt. Das Bitcoin-Netzwerk basiert auf einer sog. Blockchain, einer Datenbank, in der alle Transaktionen aufgelistet werden. Das System wird als transparenter im Vergleich zu herkömmlichen Zahlungssysteme bezeichnet, da alle Transaktionen nachvollzogen werden können. Richtig daran ist, dass sich anhand der Blockchain der Weg der Bitcoins verfolgen lässt. Da die in der Blockchain hinterlegten Adressen jedoch pseudonymisiert sind, können die dahinter stehenden Personen nicht identifiziert werden. Zur Erschwerung der Nachvollziehbarkeit wird zudem die Benutzung mehrerer Adressen empfohlen. Die für Ermittlungsbehörden spannende Frage, ob sich aus der Blockchain der Zahlungspfad nachverfolgen lässt, muss derzeit noch verneint werden.

Da der Staat aufgrund der Anonymisierung und Verschlüsselung des Bitcoin-Systems keinen Zugriff auf Zahlungsdetails erhält, eignet es sich besonders als Tätigkeitsfeld für Kriminelle, die Bitcoins überall dort einsetzen können, wo Zahlende und Empfänger anonym bleiben möchten. Bitcoins lassen sich zur Geldwäsche ebenso wie zur Zahlung von Bestechungs- und Lösegeldern und der Abwicklung illegaler Kaufgeschäfte verwenden. Aus letzteren stammen auch die beschlagnahmten 126 hessischen Bitcoins. Aber wie gelangt die Polizei in den Besitz von Bitcoins?

Beschlagnahme von Bitcoins

Sowohl das Strafprozessrecht als auch das allgemeine und (besondere, z.B. Zollrecht) Polizeirecht kennt Ermächtigungsgrundlagen zur Beschlagnahme bzw. zur Sicherstellung von Sachen. Die polizeirechtliche Befugnisnormen sprechen dem MEPOG folgend von „Sachen“, während die §§ 94, 111b, 443 StPO von „Gegenständen“ sprechen. Dies wirft die Frage nach der Rechtsnatur von Bitcoins auf. Bitcoins bestehen wie alle Kryptowährungen aus einer Kette von digitalen Signaturen, also kryptografischen Daten. Sie sind daher keine körperliche Gegenstände i.S.d. § 90 BGB. Auch können sie nicht auf einem Sparbuch oder in einem Portemonnaie aufbewahrt werden. Stattdessen unterhält jeder Nutzer einen privaten Schlüssel, mit dem er auf die Bitcoins zugreifen kann. Dieser Schlüssel kann selbst verwaltet werden. Er wird i.d.R. in einer als wallet bezeichneten digitalen Geldbörse abgespeichert. Es handelt sich um eine Software, in der der private Schlüssel hinterlegt ist, mit dem der Inhaber auf die Bitcoins zugreifen kann. Diese Speicherung kann in einem online-wallet, auf einem mit dem Internet verbundenen Gerät sogar offline auf einer sog. hardware wallet erfolgen. Der Speicherort ändert jedoch nichts an der Dateneigenschaft der Bitcoins.

Für das Strafprozessrecht ist anerkannt, dass auch Daten Gegenstand einer Beschlagnahmeanordnung sein können. Schwieriger gestaltet sich die Rechtslage im Polizeirecht, wo z.T. bereits die Beschlagnahme bzw. Sicherstellung von Forderungen und anderen Vermögensrechten mit dem Argument der Unkörperlichkeit abgelehnt wird. Andere wenden die polizeirechtlichen Normen entsprechend bzw. analog an. Zwar können Gerichte erkennbare Lücken im Gesetz in richterlicher Rechtsfortbildung schließen, doch muss bei der analogen Anwendung von Ermächtigungsgrundlagen der Eingriffsverwaltung die Analogiebildung wegen des demokratischen und grundrechtlichen Vorbehalt des Gesetzes besonders strikt gehandhabt werden. Vor allem im präventiven Polizeirecht, das anders als das Strafrecht im Tatbestand nur eine Wahrscheinlichkeitsprognose verlangt, erscheint eine Ausdehnung problematisch. Daher ist zu begrüßen, dass der baden-württembergische Gesetzgeber den Polizeivollzugsdienst nach § 33 Abs. 2 BWPOG explizit zur Beschlagnahme von Forderungen und anderen Vermögensrechten ermächtigt hat. Zwar verleiht die Verfügungsmacht über ein Bitcoin kein relatives Recht i.S.d. BGB, weil es an einer Gläubiger-Schuldner-Relation fehlt, der Wortlaut „andere Vermögensrechte“ sowohl in § 33 Abs. 2 BWPOG als auch § 111c Abs. 2 StPO ist insoweit aber offen und lässt zu, dass Kryptowährungen darunter subsumiert werden. Im Übrigen spricht auch der Telos der Normen für die erweiterte Auslegung: Sowohl das Bruttoprinzip des Verfalls als auch die Effektivität der Gefahrenabwehr bei der präventiven Sicherstellung von Vermögenswerten gebieten eine weites Verständnis.

Soweit die Bitcoins in einer hardware wallet abgelegt sind, dürften die Beschlagnahme bzw. Sicherstellung auch nach den anderen Polizeigesetzen kein Problem darstellen, da mit der Beschlagnahme bzw. Sicherstellung des Datenträgers auch die sich darauf befindlichen Daten erfasst werden.

Kein staatliches Wer-wird-Millionär-Spiel

In der Regel wird das verfügbare Bitcoin-Guthaben verteilt auf mehrere Wallets gespeichert, um das Sicherheitsrisiko zu minimieren. Wenn die Behörden die Bitcoins beschlagnahmen, ohne den zur wallet gehörenden privaten kryptografischen Schlüssel zu kennen, ist ihnen der Zugriff auf die Bitcoins verwehrt. Man kann sich dies vorstellen wie die Beschlagnahme eines Tresors, zu dem der Schlüssel oder Zugangscode fehlt und der auch sonst nicht geknackt werden kann. Daher sind die Ermittler daran interessiert, zugleich mit dem wallet auch den privaten Schlüssel sicherzustellen, um über die Bitcoins verfügen zu können. Dies ist schon deswegen erforderlich, weil es zur Sicherstellung der Bitcoins nicht ausreicht, dass die Polizei eine von möglicherweise mehreren existierenden Kopien der wallet beschlagnahmt, sondern die Bitcoins in ihren Gewahrsam verbringen muss.

Dazu können die Bitcoins nach § 111c Abs. 2 StPO gepfändet werden, wobei die Vorschriften der ZPO über die Zwangsvollstreckung in Forderungen und andere Vermögensrechte sinngemäß anzuwenden sind. Dazu sollten die Bitcoins mithilfe des privaten Schlüssels auf ein polizeiliches wallet übertragen werden. Eine sog. formlose Sicherstellung reicht hier nicht aus, da die die Bitcoins mithilfe des privaten Schlüssels und einer Internetverbindung wiederhergestellt werden können. Die Einrichtung einer polizeilichen wallet scheint auch die hessische Staatsanwaltschaft zu planen.

Kann die Polizei den privaten Schlüssel nicht sicherstellen, und kooperiert der Beschuldigte nicht mit den Ermittlungsbehörden, besteht keine Möglichkeit den Schlüssel neu zu generieren oder wiederherzustellen. Alle Bitcoins, die in Bezug zu diesem „verlorenen“ privaten Schlüssel stehen, sind praktisch für immer verloren. Auch die Fälle, in denen, etwa bei einer Hausdurchsuchung ein „offenes“ wallet gefunden wird, dürften praktisch selten sein. Um die Bitcoins weiterveräußern und wirtschaftlich nutzen zu können, ist der private Schlüssel zwingend erforderlich. Die digitalen Riesensummen, auf denen viele Ermittlungsbehörden sitzen, können daher schon technisch nur zum Teil genutzt werden. Auch dürfte eine schlagartige Veräußerung einer großen Menge Bitcoins den Kurs abstürzen lassen – sodass sich die Behörden, wie die hessische Generalstaatsanwaltschaft auf eine Anfrage hin, bedeckt halten, was Informationen über den Zeitpunkt des Verkaufs angeht.

Verkauf der Bitcoins als Notveräußerung

Dass die Bitcoins übrigens veräußert werden sollen, ist zumindest im strafrechtlichen Kontext unproblematisch. Zwar ist im Einzelnen umstritten, ob Bitcoins dem Verfall nach § 73 StGB oder der Einziehung nach § 74 StGB unterliegen, beides vollzieht sich jedoch über eine Notveräußerung nach § 111p Abs. 1 S. 1 StPO. Auf den ersten Blick erscheint verwunderlich, dass die 2014 beschlagnahmten hessischen Bitcoins erst drei Jahre später im Rahmen einer Notveräußerung verkauft werden. § 111p Abs. 1 S. 1 Var. 2 StPO sieht die Veräußerung beschlagnahmter oder gepfändeter Gegenstände auch vor, wenn andernfalls ein erheblicher Wertverlust droht. Der durch die Generalstaatsanwaltschaft Frankfurt angekündigte Verkauf der Bitcoins lässt sich daher mit den befürchteten und dann tatsächlich eingetretenen Kurseinbrüchen ab Dezember 2017 erklären. Wie hoch der

aus den 126 Bitcoins gewonnene Erlös tatsächlich ist, wird die hessische Generalstaatsanwaltschaft auf ihrer Jahrespressekonferenz voraussichtlich im März verkünden.

Veröffentlicht unter CC BY NC ND 4.0.